

다중사용자 네트워크에서 전력 제어가 기밀 용량에 미치는 영향

방인규, 정방철*, 성단근
한국과학기술원, *충남대학교

veronika@kaist.ac.kr, *bcjung@cnu.ac.kr, dksung@kaist.ac.kr

Effect of Power Control on the Secrecy Capacity in Multiuser Networks

Inkyu Bang, Bang Chul Jung*, and Dan Keun Sung

School of EE, KAIST, *Dept. of EE, Chungnam National Univ.

요약

모든 사물이 무선 인터넷으로 연결되는 사물 인터넷(internet of things) 시대를 맞이하여, 최근 무선통신분야에서는 물리계층 보안(physical layer security)이 새로운 연구 분야로 주목을 받고 있다. 본 논문에서는 다수의 악의적인 사용자들이 도청을 시도하는 다중사용자 네트워크에서 각 사용자 단말의 전력 조절(power control)이 임계값 기반의 사용자 스케줄링 방식과 결합되었을 때 기밀용량 관점에서 얻을 수 있는 성능 이득의 효과를 기존의 임계값 기반의 사용자 스케줄링 방식 그리고 최적 사용자 스케줄링 방식과 비교 분석한다.

I. 서론

오늘날, 사용자의 휴대 단말뿐만 아니라, 우리 삶을 둘러싼 다양한 사물까지 무선으로 인터넷에 연결되는 사물인터넷(internet of things) 시대를 맞이하여, 최근 무선통신분야에서는 물리계층 보안(physical layer security)이 새로운 연구 분야로 주목을 받고 있다. 무선통신에서 신호 전달의 통로로 사용되는 무선채널은 기본적으로 신호를 모든 방향으로 전달하기 때문에 도청(eavesdropping)에 매우 취약한 특성을 지닌다. 물리계층 보안은 이러한 무선채널의 취약점을 극복하여 정보이론적으로 완벽한 기밀성을 보장하는 것을 목표로 한다.

Shannon[1]과 Wyner[2]의 연구를 시작으로, 많은 연구자들이 악의적인 도청 시도가 존재하는 상황에서 무선채널을 통해 전달되는 신호의 기밀성을 보장하기 위한 연구에 집중하였다. 정보이론에 기초한 물리계층 보안 연구와 관련하여, 최근 여러 연구 주제들 중에 다중사용자 네트워크 상황에서 무선 보안 통신방법을 분석하고자하는 연구들이 많아지고 있다[3]. 다중사용자 네트워크에서, 정확한 기밀 용량(secrecy capacity)을 계산하는 것은 상당히 어렵고 복잡한 분석을 요구하기 때문에 이를 대신하여 ‘기밀 사용자 스케일링 법칙(secure user-scaling law)[4, 5]’ 그리고 ‘기밀 서비스 불능 확률(secure outage probability)[6]’ 등과 같은 근사 척도에 기초한 시스템 분석 방법을 활용한 연구들이 주목받고 있다. 특히, 기밀 사용자 스케일링 법칙은 사용자의 수와 다중사용자 다이버시티(multiuser diversity, MUD) 사이의 관계를 규명하기 위한 수학적 척도로 활용되고 있다. 기밀 사용자 스케일링 법칙과 관련된 기존 연구들[4, 5]에서는 임계값 기반의 사용자 스케줄링 방식을 사용하여, 최적 다중사용자 다이버시티(optimal MUD)를 달성하기 위한 조건을 수학적으로 규명하였다. 하지만 임계값 기반의 사용자 스케줄링 방식은 전체 사용자들 중에 임계값 조건을 만족하는 사용자 후보들을 추려내는 스케줄링 방식이기 때문에 시스템의 사용자 수가 적은 환경에서는 다중사용자 다이버시티를 온전히 활용할 수 없는 단점을 지니고 있다.

본 논문에서는 사용자 단말의 전력 조절(power control) 기법이 임계값 기반의 사용자 스케줄링 방식과 결합되었을 때 기밀용량 관점에서 얻을 수 있는 성능 이득의 효과를 분석한다.

II. 시스템 모델

본 논문에서는 N 명의 사용자와 하나의 기지국으로 구성된 단일 셀 다중 접속 환경에서 K 명의 악의적 사용자들이 도청을 시도하는 다중사용자 도청 네트워크(multiuser wiretap network)를 고려하였다. 모든 사용자들은 단일 안테나를 지니며, 악의적 사용자들은 서로 독립적으로 도청을 시도한다고 가정하였다. 하나의 전송 블록동안, 채널 값이 변하지 않는 블록 페이딩 채널 모델을 고려하였다. 또한 하나의 전송 블록동안, 한명의 사용자가 선택되어 서비스를 받는 상황을 고려하였다. 사용자 단말은 기지국 그리고 악의적 사용자로부터의 채널 정보를 얻을 수 있다고 가정하였다.

본 논문에서 h_n 과 g_{nk} 은 각각 n 번째 사용자와 기지국 그리고 n 번째 사용자와 k 번째 악의적 사용자 간의 스몰 스케일 채널 페이딩 값을 나타낸다. 분석의 편의상 라지 스케일 채널 페이딩 값은 고려하지 않았으며, h_n 과 g_{nk} 모두 평균이 0이고 공분산이 1인 복소 정규 가우시안으로 가정하였다. 이때 기지국 및 k 번째 악의적 사용자의 수신 신호는 다음과 같이 표현된다.

$$y = h_n x_n + z, \quad (1)$$

$$y_k = g_{nk} x_n + z_k, \quad (2)$$

여기서 x_n 은 최대 전송전력이 P 으로 제한되는 n 번째 사용자의 전송 심벌을 의미하며 z 과 z_k 은 평균이 0이고 공분산이 σ^2 인 복소 백색 가우시안 잡음을 나타낸다. 수식 (1)과 (2)를 바탕으로 n 번째 사용자가 스케줄링 되었을 때 얻을 수 있는 기밀 용량은 다음과 같이 표현된다.

$$C_n = \log \left(\frac{1 + |h_n|^2 \rho}{1 + \max\{|g_{n1}|^2 \rho, \dots, |g_{nK}|^2 \rho\}} \right), \quad (3)$$

여기서 ρ 는 P/σ^2 으로 정의된 송신 신호 대 잡음 비(signal-to-noise ratio, SNR)이며, 악의적 사용자들은 독립적으로 도청을 시도한다고 가정하였기 때문에 K 명의 악의적 사용자들에 의한 정보 누출(information leakage)이 K 개의 합의 형태가 아니라 K 개 중 최댓값의 형태로 나타난다.

III. 사용자 단말의 전력 조절을 고려한 스케줄링 기법

임계값 기반 스케줄링 방식[4]은 사용자와 악의적 사용자 간의 채널 상태가 임계값(η_L) 이하인 사용자만을 스케줄링 과정에서 고려하며, 정보 누출을 최소화 한다. 이는 수식으로 다음과 같이 표현된다.

$$\max\{|g_{n1}|^2, \dots, |g_{nK}|^2\} \leq \eta_L. \quad (4)$$

임계값 기반 스케줄링 방식[4]은 사용자 수가 적거나 악의적 사용자의 수가 많을 때 수식 (4)의 임계값 조건을 만족하지 못해 스케줄링 과정에서 제외되는 사용자 수가 많아진다는 단점이 있다. 따라서 사용자 단말이 전력 조절을 통해 의도적으로 정보 누출의 정도를 줄일 수 있다면 다중사용자 다이버시티를 보다 효과적으로 이용할 수 있을 것이다.

수식 (4)의 임계값 조건에 기초한 사용자 단말의 전력 조절 방법은 다음과 같이 표현된다.

$$P_n^* = \min\left\{\frac{\eta_L^*}{\max\{|g_{n1}|^2, \dots, |g_{nK}|^2\}}, 1\right\}P, \quad (5)$$

여기서 η_L^* 은 기밀 용량을 최대화를 위한 최적의 임계값이며, 이는 시뮬레이션을 통해 결정된다. 수식 (5)을 자세히 살펴보면, n 번째 사용자와 악의적 사용자들 간의 채널 값이 η_L^* 보다 클 경우에는 그 비율만큼 전송 전력이 감소하게 된다. 반대로 n 번째 사용자와 악의적 사용자들 간의 채널 값 η_L^* 보다 작아 수식 (4)의 기준을 이미 만족할 경우에는 전송 전력은 최대 전송 전력 값 P 가 된다. 또한 제안 스케줄링 기법은 최적 다중사용자 다이버시티를 달성할 수 있다. (본 논문에서 이에 대한 수학적 증명은 생략한다.)

IV. 시뮬레이션 결과 및 결론

본 논문에서는 제안 스케줄링 기법의 성능을 평가하기 위해 3가지 기법을 고려하였다. SILR(signal-to-information leakage ratio)은 사용자의 신호 대 정보누출 비율을 스케줄링 척도로 삼은 스케줄링 기법이며, 단일 셀 환경에서는 기밀 용량 관점에서 최적의 결과를 의미한다. TS(threshold-based scheduling)은 기존의 연구결과[4, 5]에서 고려하고 있는 임계값 기반의 스케줄링 기법이다. 마지막으로 MaxSNR은 사용자와 기지국간의 채널만을 고려한 스케줄링 기법이다. 제안 기법은 TSPC(threshold-based scheduling with power control)으로 명명하였다. 시뮬레이션 환경으로 사용자가 적고 ($N=30$) 악의적 사용자가 다소 많은 ($K=5$) 환경을 고려하였다. 그림 1과 그림 2는 각각 사용자 수 혹은 송신 SNR 변화에 따른 평균 기밀 데이터율을 보여준다.

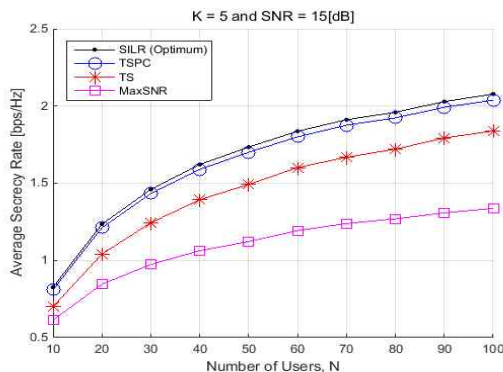


그림 1. 사용자 수 변화에 따른 평균 기밀 데이터율

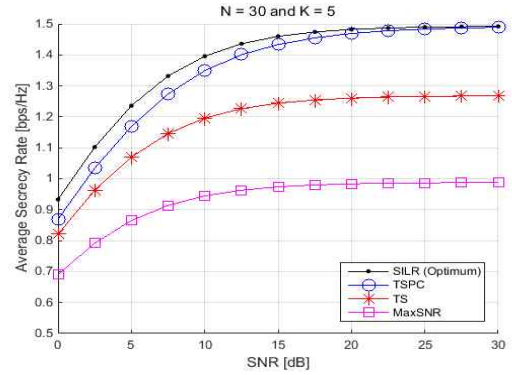


그림 2. 송신 SNR 변화에 따른 평균 기밀 데이터율

두 결과그래프에서 모두 TSPC 기법이 기존의 TS 기법과 MaxSNR 기법의 성능을 압도하는 것을 확인할 수 있다. 또한 TSPC 기법은 단일 셀 환경에서 최적의 결과인 SILR 결과와 거의 비슷한 성능을 지니는 것을 확인할 수 있다. 그림 1을 살펴보면 MaxSNR 기법은 사용자와 악의적 사용자 간의 채널을 고려하지 않은 스케줄링 기법이기 때문에 사용자 수가 증가 할수록 성능 차이가 확연해진다. 반면 TSPC 기법과 TS 기법의 성능 차이는 거의 동일하게 유지된다. 그림 2를 살펴보면 그림 1과는 반대로 SNR 값이 커짐에 따라 TSPC 기법과 TS 기법의 성능 차이가 커지는 것을 확인할 수 있다. 이는 SNR 값이 커질수록 수식 (4)에 의해 제외되는 사용자들로 인한 다중사용자 다이버시티 이득이 커지기 때문이다.

본 논문에서는 단일 셀, 단일입출력 환경에서 사용자 단말의 전력 조절이 기밀 용량에 미치는 영향을 분석하였다. 사용자 단말의 전력 조절은 네트워크의 사용자 수가 적거나 악의적 사용자가 많은 환경에서 다중사용자 다이버시티 이득을 극대화 시킨다.

ACKNOWLEDGMENT

This work has been supported by the National GNSS Research Center program of Defense Acquisition Program Administration and Agency for Defense Development.

참 고 문 헌

- [1] C. E. Shannon, "Communication theory of secrecy systems," Bell Syst. Tech. J., vol. 28, pp. 656 - 715, Oct. 1949
- [2] A. D. Wyner, "The wire-tap channel," Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355 - 1387, Oct. 1975.
- [3] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," IEEE Commun. Surveys Tuts., vol. 16, no. 3, pp. 1550 - 1573, Third Quarter, 2014.
- [4] H. Jin, W. Y. Shin, and B. C. Jung, "On the multi-user diversity with secrecy in uplink wiretap networks," IEEE Commun. Lett., vol. 17, no. 9, pp. 1778 - 1781, Sept. 2013.
- [5] I. Bang, S. M. Kim, and D. K. Sung, "Effects of multiple antennas and imperfect channel knowledge on secrecy multiuser diversity," IEEE Commun. Lett., vol. 19, no. 9, pp. 1564 - 1567, Sept. 2015.
- [6] Y. Zou, X. Li, and Y.-C. Liang, "Secrecy outage and diversity analysis of cognitive radio systems," IEEE J. Sel. Areas Commun., vol. 32, no. 11, pp. 2222 - 2236, Nov. 2014.